UNIWERSYTET JAGIELLOŃSKI
DO-0130/29/2006

Zarządzenie nr 29
Rektora Uniwersytetu Jagiellońskiego
z 24 marca 2006 roku

w sprawie: wprowadzenia *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Jagiellońskim*

Na podstawie § 8 ust. 1 zarządzenia nr 14 Rektora Uniwersytetu Jagiellońskiego z 10 lutego 2006 roku w sprawie ochrony danych osobowych przetwarzanych w UJ zarządzam, co następuje:

§ 1

Wprowadza się ***Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Jagiellońskim***, stanowiącą załącznik do niniejszego zarządzenia.

§ 2

1. ***Instrukcja***, o której mowa w § 1, stanowi podstawę do opracowania instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe przez lokalnych administratorów bezpieczeństwa informacji w konkretnej jednostce organizacyjnej.
2. ***Instrukcja***, o której mowa w § 1, wraz z załącznikiem stanowić będzie zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Jagiellońskim.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

Prof. dr hab. Karol Musioł

Otrzymują:

- **Prorektorzy**
- **Dziekani Wydziałów**
- **Dyrektorzy/Kierownicy jednostek poza- i międzywydziałowych oraz międzyuczelnianych**
- **Kanclerz UJ**
- **Z-ca Dyrektora Adm. UJ ds. Collegium Medicum**
- **Z-ca Dyrektora Adm. UJ. ds. Teleinformatycznych**
- **Sekcja Ochrony Informacji Niejawnych i Spraw Obronnych**
- **Dział Spraw Osobowych (+ Collegium Medicum)**
- **Dział Nauczania**
- **Zespół Radców Prawnych**

Załącznik
do zarządzenia nr 29 Rektor UJ
z 24 marca 2006 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Jagiellońskim

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie teleinformatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Rejestracja, wyrejestrowanie lub zmiana uprawnień użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego danego pracownika, po zatwierdzeniu przez lokalnego administratora danych osobowych.
2. Uprawnienia do realizacji powyższych czynności posiada lokalny administrator bezpieczeństwa informacji.
3. Lokalny administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji pracowników, w formie elektronicznej i tradycyjnej, dopuszczonych do pracy w systemie informatycznym przetwarzającym dane osobowe.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm haseł jako narzędzie umożliwiające bezpieczne uwierzytelnienie. Za przydzielenie tymczasowego hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada lokalny administrator bezpieczeństwa informacji. Za wygenerowanie hasła odpowiada lokalny administrator bezpieczeństwa informacji.
2. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymuszający bezpieczne zarządzanie hasłami użytkowników, z tego względu:
   - hasło tymczasowe przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe;
   - hasła są zmieniane przez użytkowników;
   - system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła;
   - system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, w szczególności hasło powinno składać się z co najmniej ośmiu przypadkowych znaków, zawierać co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny;
   - wprowadzone hasło powinno różnić się od, co najmniej, trzech ostatnio stosowanych, przy czym system informatyczny jest wyposażony w mechanizmy pozwalające na wymuszenie wymaganych różnic;
   - system informatyczny posiada mechanizmy automatycznego generowania przez administratora systemu informatycznego haseł dla użytkownika, który może być włączony w uzasadnionych przypadkach, na wniosek lokalnego administratora bezpieczeństwa informacji.

3. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasła. Zasady zarządzania hasłami są analogiczne, jak w przypadku zwykłych haseł użytkowników.
4. Za ochronę krytycznych elementów systemu, np. serwera bazy danych, miejsc przechowywania kopii itd. odpowiada lokalny administrator bezpieczeństwa informacji.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
2. Użytkownik powinien powiadomić lokalnego administratora bezpieczeństwa informacji lub inne osoby przez niego upoważnione, zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych, jeżeli:
   - wygląd aplikacji odbiega od stanu normalnego;
   - pewne opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też pewne opcje, niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne;
   - sposób działania aplikacji znacząco odbiega od normalnego stanu;
   - zakres danych lub sposób ich przedstawienia przez aplikację odbiega od stanu normalnego.
3. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.
4. Użytkownik może przetwarzać dane osobowe w systemie komputerowym w godzinach pracy. Przetwarzanie danych osobowych po godzinach pracy wymaga zgody przełożonego oraz powiadomienia lokalnego administratora bezpieczeństwa informacji.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii awaryjnych. Za określenie procedury tworzenia kopii awaryjnych odpowiada lokalny administrator bezpieczeństwa informacji. Do tworzenia kopii awaryjnych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego.
2. Lokalny administrator bezpieczeństwa informacji, w porozumieniu z lokalnym administratorem danych osobowych, jest odpowiedzialny za tworzenie i przekazywanie użytkownikom grafiku określającego kto i kiedy – w jakie dni i w jakich godzinach tworzy kopie awaryjne.
3. Lokalny administrator danych osobowych przeprowadza raz na sześć miesięcy testy odtworzeniowe kopii awaryjnych, sporządzając protokół potwierdzający ich wykonanie.
4. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają niszczeniu zgodnie z obowiązującymi wytycznymi.

5. Sposoby, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

1. Nośniki danych osobowych, zarówno w postaci elektronicznej jak i tradycyjnej, winny być zabezpieczone przed dostępem osób nieupoważnionych. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii awaryjnych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2. Lokalny administrator bezpieczeństwa informacji prowadzi ewidencję nośników przenośnych. Ewidencja sporządzana jest w celu zapewnienia rozliczalności procesów przetwarzania informacji w systemie informatycznym przetwarzającym dane osobowe.
3. Przekazywanie nośników danych osobowych i wydruków poza obręb jednostek organizacyjnych uczelni odbywa się za wiedzą i zgodą lokalnego administratora danych osobowych.
4. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika albo usunięcie danych z nośnika.
5. Kopie zapasowe oraz wydruki z danymi osobowymi są oznaczane, przechowywane, niszczone i archiwizowane zgodnie z wytycznymi zawartymi w Instrukcji Kancelaryjnej Uczelni.

6. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest nieuprawniony dostęp do systemu informatycznego

1. Lokalny administrator bezpieczeństwa informacji jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.
2. System antywirusowy powinien być skonfigurowany w następujący sposób:
   - skanowanie dysków zawierających potencjalnie niebezpieczne kody przy włączeniu komputera – raz dziennie;
   - skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.
3. Lokalny administrator bezpieczeństwa informacji jest odpowiedzialny za aktualizację wzorców wirusów. System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
4. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator bezpieczeństwa informacji winien podjąć działania zmierzające do usunięcia zagrożenia.

7. Procedura wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych osobowych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe mogą być wykonywane wyłącznie przez firmy, z którymi została podpisana stosowna umowa normująca w szczególności zasady ochrony danych.

2. Użytkownicy systemu winni zgłaszać niesprawności systemu informatycznego lokalnemu administratorowi bezpieczeństwa informacji lub lokalnemu administratorowi danych osobowych, którzy są uprawnieni do kontaktów z firmą serwisową.
3. Lokalny administrator bezpieczeństwa informacji może wyznaczyć osoby upoważnione do nadzorowania i odbioru wszystkich napraw systemu informatycznego lub do nadzorowania wszystkich napraw określonych komponentów systemu.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza jednostką organizacyjną Uczelni dane z naprawianego urządzenia muszą zostać usunięte zgodnie ze szczegółowymi wytycznymi. Od powyższego wymagania możliwe jest odstępstwo, jeżeli urządzenie, podczas przechowywania poza jednostką organizacyjną Uczelni, będzie pod stałym nadzorem osoby upoważnionej do dostępu do danych na nim przetwarzanych.
5. Lokalny administrator bezpieczeństwa informacji prowadzi rejestr prac serwisowych i konserwacyjnych, wykonanych w zakresie systemu informatycznego przetwarzającego dane osobowe.
6. Lokalny administrator bezpieczeństwa informacji w porozumieniu użytkownikiem systemu jest odpowiedzialny za okresowy przegląd zbioru danych osobowych oraz usunięcie danych, których przechowywanie jest dłużej nieuzasadnione.

8. Sposób realizacji wymogów w zakresie udostępniania danych osobowych odbiorcom

Lokalny administrator danych osobowych odnotowuje fakt udostępnienia informacji o danych osobowych (komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione).

Uwaga!
Załącznik do niniejszej Instrukcji stanowi przykład, który należy dostosować do specyfiki jednostki organizacyjnej i posiadanego systemu komputerowego.

Sporządzając instrukcję należy kierować się następującymi wskazówkami:

a. punkty wytłuszczone pozostawić bez zmian;
b. w tytule instrukcji należy określić nazwę bazy oraz jednostkę w której dana baza się znajduje;
c. w punkcie 1.1. należy podać stanowisko osoby zgodnie z § 5 zarządzenia nr 14 Rektora UJ z 10 lutego 2006 roku;
d. w punkcie 1.3 należy podać stanowisko osoby która w danej jednostce pełni funkcję lokalnego administratora bezpieczeństwa informacji;
e. punkcie w 4.1 należy podać zakres czasowy w jakim maja zostać archiwizowane dane.

W razie wątpliwości informacji udziela Z-ca Dyrektora ds. teleinformatycznych:

dr Józef Oleszkiewicz, tel. w. 1498, 1499, tel. 0-12-663-14-98, 0-12-663-14-99, kom. 0506 006-640, a w sprawach Collegiim Medicum: kierownik Ośrodka Komputerowego CM UJ mgr inż. Lucjan Stalmach, 012-422-99-63, kom. 0607 628-889.

Załącznik do *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w UJ*, wprowadzonej zarządzeniem nr 29 Rektora UJ z 24 marca 2006 r.

Instrukcja zarządzania systemem informatycznym

w zakresie danych osobowych .....
.....
.....

1. **Procedury związane z nadawaniem uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie teleinformatycznym oraz wskazanie osoby odpowiedzialnej za te czynności:**
   1.1. Pełne uprawnienia do systemu nadaje ..... Jest to Lokalny Administrator Danych Osobowych (LADO).
   1.2. Pełnomocnik Lokalnego Administratora Danych Osobowych lub Lokalny Administrator Danych Osobowych powołuje użytkowników systemu informatycznego którzy mają uprawnienia do przetwarzania danych osobowych w systemie. Rejestr użytkowników jest prowadzony na podstawie Zarządzenia nr 14 Rektora UJ z dnia 10 lutego 2006 i załącznika nr 4 do tego zarządzenia
   1.3. Lokalnym Administratorem Bezpieczeństwa Informacji jest:
   .....
   1.4. Jest prowadzony i uaktualniany rejestr uprawnień przyznanych poszczególnym osobom do elementów systemu oraz przetwarzania i rejestrowania danych osobowych.

2. **Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem:**
   2.1. W celu wejścia na obszar, w którym wprowadzane i przetwarzane są dane osobowe, wydaje się pracownikom odpowiednie upoważnienia na piśmie.
   2.2. Uzyskanie dostępu do systemu przetwarzania i wprowadzania danych osobowych następuje poprzez podanie prawidłowego identyfikatora i hasła przyznanych przez administratora – lub identyfikatora i Hasła automatycznie wygenerowanego przez system. Hasło nadane przez administratora musi składać się z co najmniej 8 znaków, zawierając małe i duże litery oraz cyfry a także znaki interpunkcyjne. Zmiana hasła następuje nie rzadziej niż co 30 dni.
   2.3. Użyty identyfikator nie może być powtórnie przyznany innemu użytkownikowi.
   2.4. Użytkownik któremu przypisano identyfikator i hasło zobowiązany jest do przestrzegania następujących zasad:
      - Powierzony identyfikator i hasło nie może znajdować się w miejscu widocznym dla osób nieupoważnionych (np. zawieszone na monitorze);
      - Niedopuszczalne jest uwierzytelnianie się („logowanie się") na identyfikator i hasło innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika. Zabrania się również udostępniania przydzielonego osobistego Identyfikatora i Hasła innym użytkownikom a także osobom nieupoważnionym;
      - W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie) lub działania systemu, użytkownik niezwłocznie powiadamia o nich Lokalnego Administratora Bezpieczeństwa informacji, który ma obowiązek zapoznać się z przekazanymi uwagami oraz podjąć odpowiednie działania opisane w punkcie 6.2.;
      - Użytkownicy systemu zobowiązani są do ochrony wprowadzanych danych przez zabezpieczenie ekranu monitora przez wzrokiem nieupoważnionych osób. Niedopuszczalna jest sytuacja, gdy ekran monitora osoby wprowadzającej dane skierowany jest w stronę osób nieupoważnionych;
      - Po zakończeniu operacji w systemie użytkownik obowiązany jest wylogować się z systemu;
      - W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych każdy z użytkowników obowiązany jest niezwłocznie powiadomić o tym Lokalnego Administratora Bezpieczeństwa.
   2.5. Przesyłanie identyfikatorów oraz haseł do systemu zdalnego odbywa się przy zastosowaniu algorytmów szyfrujących zaimplementowanych w kliencie przesyłania danych. Dopuszczalne jest korzystanie ze zwykłej przeglądarki internetowej, pod warunkiem że dane zostaną zaszyfrowane i przesłane do systemu zdalnego za pomocą np. protokołu SSL.

3. **Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:**
   3.1. Użytkownik rozpoczyna pracę w systemie od następujących czynności:
      - włączenia komputera,
      - uwierzytelnienia się („zalogowania się") w systemie poprzez podanie Identyfikatora i Hasła.
   3.2. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności nośniki danych (dyskietki, płyty CD, DVD), dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
   3.3. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszasz ekranu z opcją ponownego „logowania" się do systemu.

4. **Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:**
   4.1. Pełne kopie zapasowe danych osobowych ..... wykonywane są raz na ..... i po zaszyfrowaniu przesyłane na zdalne systemy. Raz na ..... wykonywany jest zapis najnowszej wersji kopii zapasowej na zewnętrznym nośniku ..... . Po upływie ..... kopie zapasowe są niszczone w sposób uniemożliwiający jakikolwiek odczyt danych na nich zawartych.
   4.2. Kluczami szyfrującymi, umożliwiającymi dostęp do kopii zapasowych dysponują wyłącznie osoby z listy w punkcie 1.1.
   4.3. Kopie zapasowe przechowywane są w ściśle określonym, chronionym miejscu do którego mają dostęp tylko upoważnione osoby z listy w punkcie 1.1. Miejsce to powinno być różne od miejsca przechowywania zbiorów danych, z których sporządzono kopie zapasowe.

5. **Procedury niszczenia nośników zawierających informacje z bazy danych osobowych po zakończeniu okresu ich użytkowania:**
   5.1. Dyski Twarde, których wskutek uszkodzenia nie da się uruchomić w serwerze lub stacji roboczej niszczy się poprzez:
      - Uderzenie - zmiażdżenie młotkiem układów scalonych na płytce sterującej dyskiem;
      - Dokonanie otworów za pomocą wiertarki we wszystkich tarczach dysku twardego w sposób asymetryczny.
   5.2. Dyski Twarde które po zakończeniu eksploatacji da się uruchomić niszczy się w sposób opisany w punkcie 5.1 lub stosuje się program do nadpisywania danych na całym obszarze przestrzeni dyskowej, który skutecznie uniemożliwi odczyt poprzednich danych zawartych na dysku.
   5.3. Nośniki kopii zapasowych, po zaprzestaniu ich użytkowania, należy pozbawić danych i zniszczyć w sposób uniemożliwiający ich użycie.
   5.4. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby nieuprawnione. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

6. **Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest nieuprawniony dostęp do systemu informatycznego:**
   6.1. Sprawdzanie obecności wirusów komputerowych oraz programów, których celem jest nieuprawniony dostęp do systemu, dokonywane jest poprzez zainstalowanie oprogramowanie antywirusowe, który skanuje automatycznie bez udziału użytkownika komputer/terminal. Program jest zainstalowany na wszystkich serwerach i stacjach roboczych.
   6.2. Podczas uruchomienia systemu program powinien sprawdzać wersję posiadanego programu antywirusowego i w razie konieczności dokonać automatycznej aktualizacji do najnowszej wersji.
   6.3. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.
   6.4. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

7. **Postępowanie w przypadku stwierdzenia naruszenia ochrony danych osobowych**
   7.1. Każda osoba zatrudniona w jednostkach organizacyjnych UJ wprowadzających dane do systemu, która stwierdza lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie, powinna niezwłocznie poinformować o tym Lokalnego Administratora Bezpieczeństwa Informacji.
   7.2. Po stwierdzeniu naruszenia Lokalny Administrator Bezpieczeństwa Informacji powinien:
      - zapisać wszelkie informacje związane z danym zdarzeniem, a szczególnie dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych,
      - na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
      - przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych,

- niezwłocznie podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów ingerencji.

7.3. Po wyeliminowaniu bezpośredniego zagrożenia Lokalny Administrator Bezpieczeństwa Informacji powinien przeprowadzić wstępną analizę stanu systemu w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie oraz sprawdzić:
- stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
- zawartość zbioru danych osobowych,
- poprawność działania programu.

7.4. Lokalny Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Bezpieczeństwa Informacji oraz Lokalnemu Administratorowi Danych Osobowych szczegółowy raport o przyczynach, przebiegu i wnioskach wynikających ze zdarzenia. Dalsze dodatkowe czynności podejmuje po otrzymaniu ewentualnych dodatkowych poleceń od Administratora Bezpieczeństwa Informacji i Lokalnego Administratora Danych Osobowych.

8. **Sposób realizacji wymogu rejestracji informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia:**

8.1. Użytkownik zapisuje w rejestrze prowadzonym w formie papierowej informacje o odbiorcach danych osobowych w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

9. **Procedura wykonania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:**

9.1. Przeglądy i konserwacje systemu i zbiorów wykonywane są na bieżąco, lecz nie rzadziej niż raz w miesiącu. Sprawdzona zostaje spójność danych, indeksów oraz stan nośników np. dysków twardych.

9.2. Okresowo (nie rzadziej niż raz na miesiąc) sprawdzona zostaje możliwość odtworzenia danych z kopii zapasowej.

9.3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których wiarygodność fachowego wykonania usługi oraz wiarygodność finansowa zostały sprawdzone na rynku.

9.4. Naprawy serwisowe sprzętu objętego umowami serwisowymi odbywać się będą zgodnie z zasadami ustalonymi w umowie serwisowej.

9.5. Naprawa sprzętu, która odbywa się w miejscu jego użytkowania, wymaga nadzoru osób użytkujących sprzęt.

9.6. Sprzęt komputerowy przed oddaniem do serwisu poza miejsce jego użytkowania, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki, a z dysków twardych skutecznie usunąć zbiory danych i programy specjalistyczne. Niedopuszczalne jest przekazanie do naprawy poza siedzibę Uniwersytetu Jagiellońskiego uszkodzonego elementu, na którym są przechowywane dane chronione.

9.7. Zmiana konfiguracji sprzętu komputerowego lub zmiana jego lokalizacji może być dokonana tylko za zgoda lokalnego administratora bezpieczeństwa informacji.

Podpis Lokalnego Administratora Danych Osobowych (lub Jego pełnomocnika)

.....